Surveillance Technology and How Police Are Using It

Blake Feldman

Fall Public Defender Conference

October 27, 2016

Historical Insight

" . . . under ordinary and normal circumstances wire-tapping by government agents should not be carried on for the excellent reason that it is almost bound to lead to abuse of civil rights."

- **President Franklin D. Roosevelt (1940)**

"Drug arrests are disproportionately black ***because of police department surveillance patterns***. [S]tudies prove that our drug enforcement efforts result in black city-dwellers being disproportionately arrested for activity both races engage in, simply because they are more easily subject to surveillance."

- **Judge Robert L. Carter (2000)**

Surveillance has been used by governments throughout history to suppress free speech and intimidate the leaders of political movements.

Civil Rights Leaders:

- *The Nation*'s Betty Medsger reported that under J. Edgar Hoover, who led the FBI for 48 years, " . . . directives [] required FBI field offices to watch African-Americans wherever they went—in churches, in classrooms, on college campuses, in bars, in restaurants, in bookstores, in their places of employment, in stores, in any social setting, in their neighborhoods and even at the front doors of their homes."

Black Lives Matter:

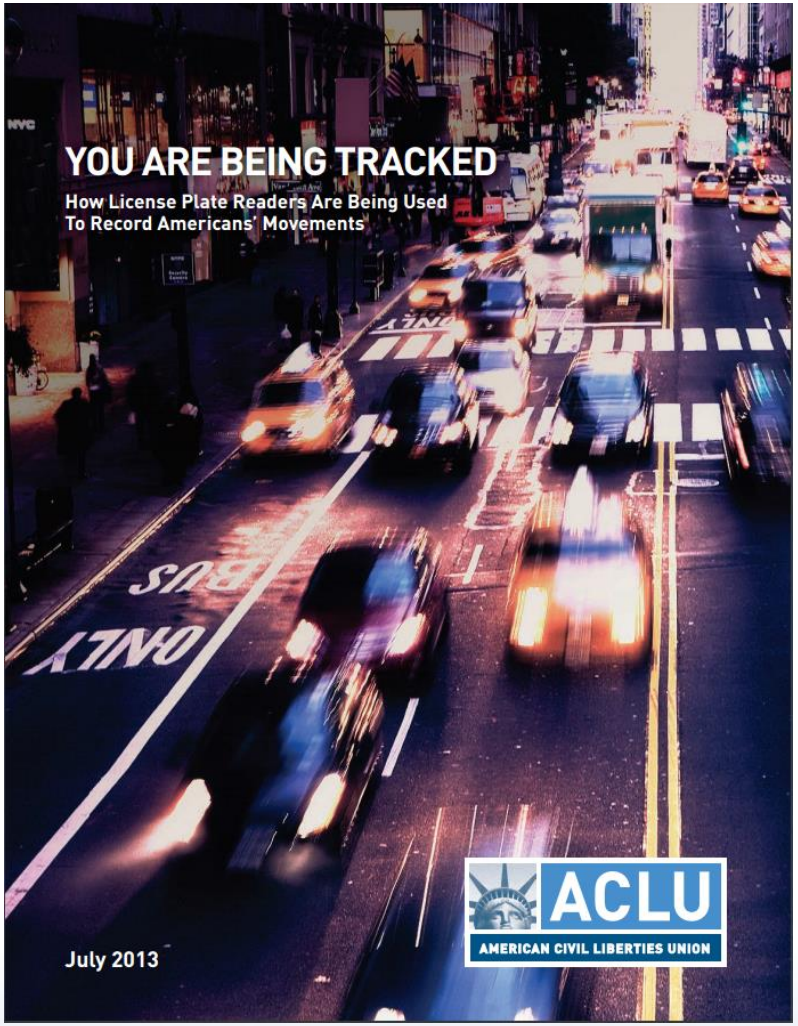
- NYPD systemically surveilling Muslims since 0/11
- Chicago PD systemically surveilling meetings post-Ferguson.
- Sophisticated aerial surveillance of Baltimore protests.

Surveillance Technology

An Overview

- Common Types of Surveillance Technology
  - What the technology does
  - Why the ACLU is concerned

Automatic License Plate Readers



- **Function(s):** ALPRs (fixed or mobile) take photographs of license plates, digitize them, and enable the captured data to be searched, stored or processed in real time or historically.

ACLU
AMERICAN CIVIL LIBERTIES UNION of MISSISSIPPI

Automatic License Plate Readers

- **Issue(s):**
  - **Retention:** The data collected by them, which should in the absence of a warrant be processed and deleted in matter of days, is often kept for months or even years. This allows the government to track where people travel in their cars
  - **Privatization:** Private companies providing ALPRs to localities free of charge in return for access to the data they collect, which they then monetize
  - **Unknown:** Due to a lack of data, it is hard to ascertain if ALPRs are being deployed discriminatorily.

Closed-Circuit Television Cameras

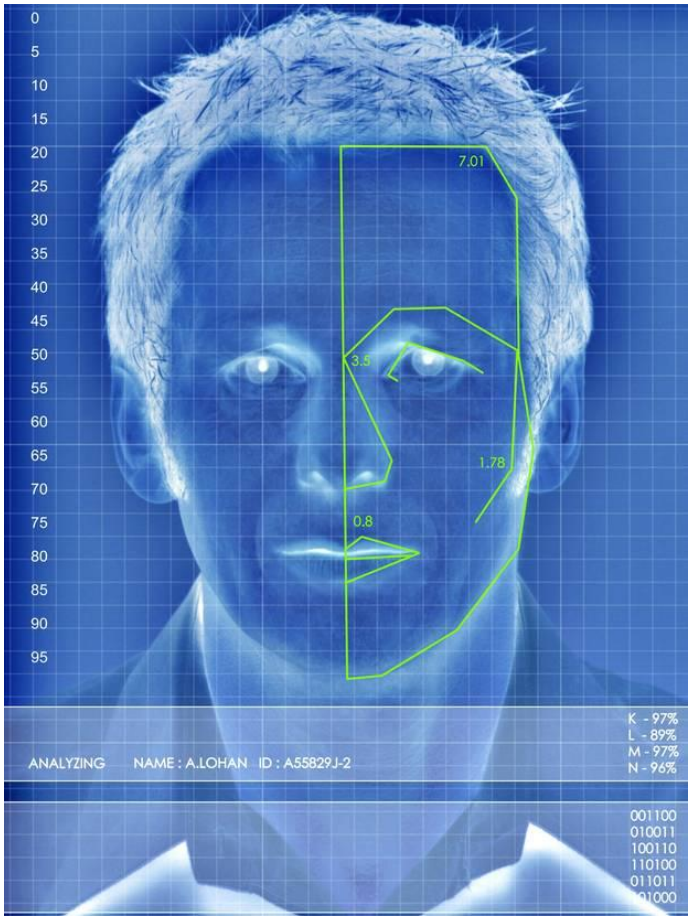
- **Function(s):** CCTV cameras are video cameras that transmit their signal to a limited number of external monitors or computers. They are frequently used by the police to monitor public spaces remotely. CCTV is also widely used by private entities for security and monitoring purposes.

Closed-Circuit Television Cameras

- **Issue(s):**
  - CCTV allows police to monitor public activities virtually 24/7 without a real justification or public benefit.
  - The cameras are over-deployed in areas that are deemed by police to be “high crime,” which often really means communities of color.
  - A growing area of concern is with police departments seeking to voluntarily gain remote access to private CCTV systems.
  - We are also increasingly concerned about the placement of cameras directly outside of private homes.

Biometric Surveillance Technology

- **Function(s):** These technologies allow a person to be identified using a physical trait (e.g., fingerprints, DNA, facial features, voice, iris, gait).



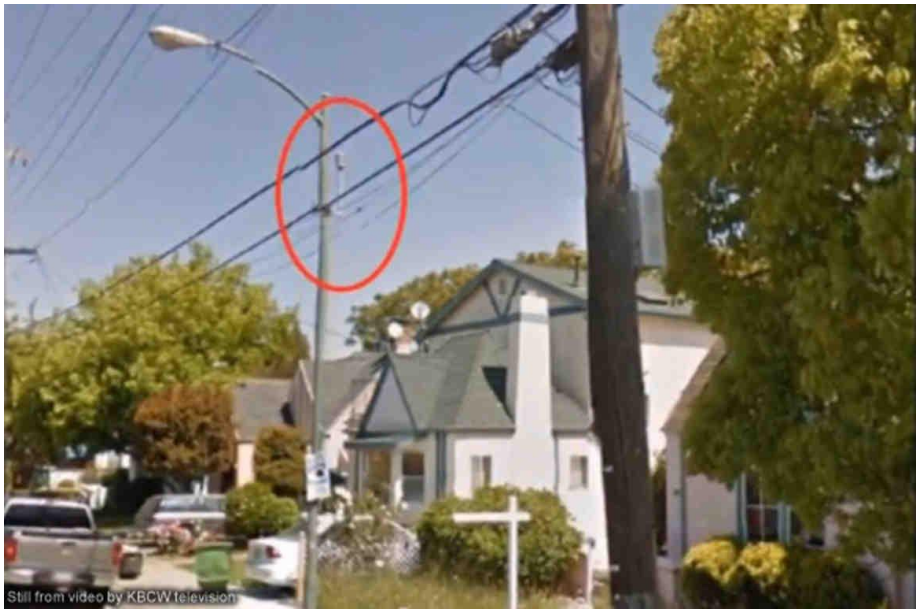
ACLU
AMERICAN CIVIL LIBERTIES UNION of MISSISSIPPI

Biometric Surveillance Technology

- **Issue(s):**
  - This is no longer limited to fingerprints and DNA, which could only be obtained voluntarily or following an arrest.
  - It completely undermines the ability of person to travel in public or gather with friends anonymously
  - These systems are imperfect, which can produce a lot of false-positives that result in innocent people unjustifiably drawing the attention of law enforcement.
  - Due to technological limitations and biased engineering practices, these false-positives are far more likely to occur with non-whites than with whites.

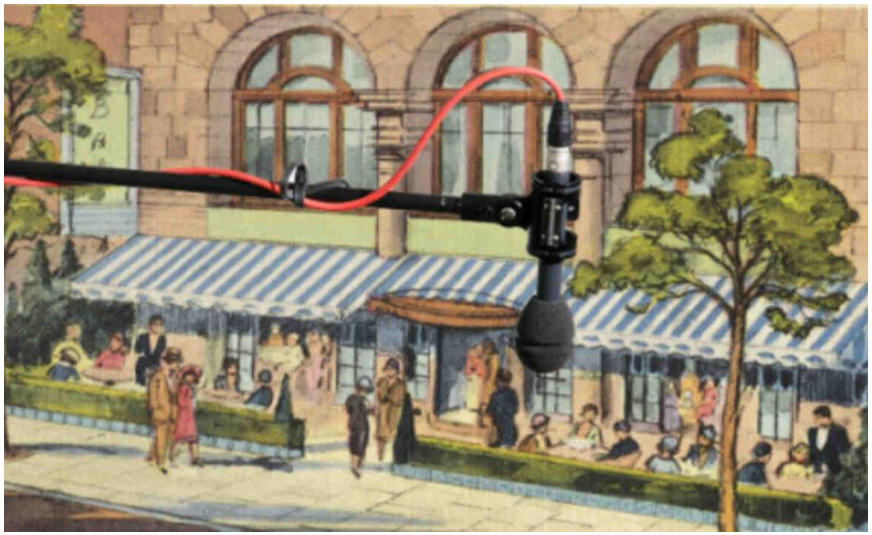
Gunshot detection and location hardware and services

- **Technology Name(s):** ShotSpotter
- **Function(s):** Gunshot detectors, like ShotSpotter, and essentially microphones that are designed to detect the sound of a gunshot. By placing them throughout an area, the microphones are able to triangulate a gunshot and provide police with a limited geographic location from which a gunshot emanated.



Gunshot detection and location hardware and services

- **Issue(s):** If these secretly operated microphones can be remotely activated and used to listen in on the communities in which they are placed, they can represent another form of general, mass surveillance.



Only with strict limitations and auditing can we be sure this technology is not abused, and such oversight commonly does not exist.

X-ray Vans

- **Technology Name(s):** Z Backscatter Vans
- **Function(s):** The technology, much like the now retired backscatter machines used by TSA at airport security checkpoints, uses x-ray radiation to do what no human eye can do, like see through clothing and car exteriors.

X-ray Vans

- **Issue(s):** We don't know exactly how government purchasers of these vans are using them, but if they are in fact being used on public streets in non-emergencies and without a warrant, that would be a major violation of the Constitution (not to mention a possible threat to public health).

  Unless they have probable cause to search a specific vehicle, government agencies should not be roaming U.S. streets conducting backscatter X-ray scans of vehicles and their occupants (much less pedestrians, cyclists, etc.) without their knowledge or consent.

Surveillance Enabled Lightbulbs

- **Function(s):** While posing as energy efficient upgrades to existing incandescent lightbulbs, LED surveillance lightbulbs actually conceal tiny cameras and microphones that can stealthy monitor their surroundings and transmit their feeds back to a central monitoring station or computer.

Surveillance Enabled Lightbulbs

- **Issue(s):**
  - LED surveillance lightbulbs, if installed on municipal streetlamps, would throw a net of almost unprecedented scope over entire communities or cities.
  - What is particularly troubling with surveillance bulbs is the stealthy way in which they are being marketed and pitched to the press; to wit, as an energy efficient light bulb with built-in monitoring technology.
  - What the product really appears to be is a mass surveillance device being disguised as an LED light bulb.

Hacking Software and Hardware

- **Function(s):** This technology allows law enforcement to access a person's personal computing equipment (including desktops, laptops, cell phones, tablets, etc.) or password-protected websites or accounts (such as cloud storage or a social media account), either in person or remotely, without the permission of either the account-holder or the operator of the service.

Hacking Software and Hardware

- **Issue(s):**
  - When a government hacks into a private computer or account, is does so with the specific intent of surveilling the private contents of that computer or account without the person's permission or knowledge.
  - Hacking tools depend on vulnerabilities that can be targeted by criminals as well as law enforcement. A government that invests in hacking tools has a perverse incentive to avoid shoring up the infrastructure the public depends on, weakening its role as a promoter of the public good.

Social Media Monitoring Software (SMMS)

- **Technology Name(s):**
  - Digital Stakeout
  - XI Social Discovery
  - Geofeedia
  - Dataminr
  - Dunami
  - SocioSpyder

Social Media Monitoring Software (SMMS)

- **Function(s):**
  - covertly monitor, collect, and analyze individual's social media data from platforms like Twitter, Facebook, and Instagram.
  - perform highly sophisticated fishing expeditions across the internet by using complex algorithms to analyze/organize data.
  - geographically track people as they communicate.
  - chart people's relationships, networks, and associations.
  - monitor protests, identify the leaders of political and social movements, and measure a person's influence.
  - It is also promoted as a predictor of future events, including threat assessment, and as an instrument for manipulating public opinion.

Social Media Monitoring Software (SMMS)

- **Issue(s):**
  - SMMS improperly blankets a whole range of innocent people without any evidence of wrongdoing.
  - SMMS has the potential to chill free speech.
  - The imprecise and privacy-violating manner in which it sweeps in the postings of scores of innocent people, and the degree to which it is over-focused on persons of color, has earned it the description of a “21st century stop and frisk.”
  - SMMS has been used extensively and aggressively against Black Lives Matter leaders and protestors.

Surveillance has been used by governments throughout history to suppress free speech and intimidate the leaders of political movements.

Civil Rights Leaders:

- The FBI and NSA routinely spied on civil rights leaders including Martin Luther King Jr. and Cesar Chavez. The FBI used information from secret surveillance of civil rights leaders to discredit and intimidate them.

Black Lives Matter:

- Fresno, CA police have for years systematically monitored social media activity related to the BLM movement.
- An investigator at the Oregon DOJ racially profiled Twitter users using the hashtag #BlackLivesMatter.
- A cybersecurity firm with ties to law enforcement monitored prominent BLM leaders and labeled them “threat actors.”

Through-the-wall Sensors/Radar

- **Function(s):** This technology uses radar or similar technology to peer through to walls of a building.
  - Currently the technology is precise enough to ascertain how many people are in a particular room within a dwelling unit.
  - Over time, the clarity of the image produced by wall-penetrating technologies may become precise enough to determine the identities of a building's occupants.

Through-the-wall Sensors/Radar

- **Issue(s):**
  - While this technology may have beneficial uses, such as allowing a SWAT team to learn the number of occupants in a home, and whether or not they are armed, prior to a raid, any such use is only appropriate pursuant to a warrant.
  - Because this technology can be use stealthy, and as it advances, it may increasing (and improperly) be used as a way to looking into private swellings without court oversight.

Body-worn Cameras

- **Function(s):** BWCs are intended to capture police interactions with the public from an angle approximating a police officer's point of view. .
- **Issue(s):** While wearable cameras have the potential to provide greater police transparency and accountability, they can also present a significant threat to privacy.
  - With the wrong policies in place, body cameras can be turned from a transparency and accountability tool into a police propaganda and mass surveillance tool.

Predictive Policing Software

- **Function(s):**
  - Predictive policing software uses mathematical and analytical techniques to attempt to predict future criminal activity (a sci-fi version of its use is the basis for the film “Minority Report”).
  - Predictive policing software is claimed to be helpful in predicting crimes, predicting offenders, predicting perpetrators’ identities, and predicting victims of crime.

Predictive Policing Software

- **Issue(s):**
  - Inputting historically biased data into a computer and then crunching it through an algorithm will merely produce biased results that instruct the police to continue to over-police poor communities and communities of color.
  - This highly untested technology raises numerous additional questions, including how accurate the algorithms are in extracting information from data.
  - These tools are often proprietary, with algorithms, data inputs, and source code shielded from review or oversight.

Stingrays

The Most Common Surveillance Tool the Government Won't Tell You About

- What are they?
- Why the ACLU is concerned?
- Who has them?
- A Guide For Criminal Defense Attorneys

Stingrays

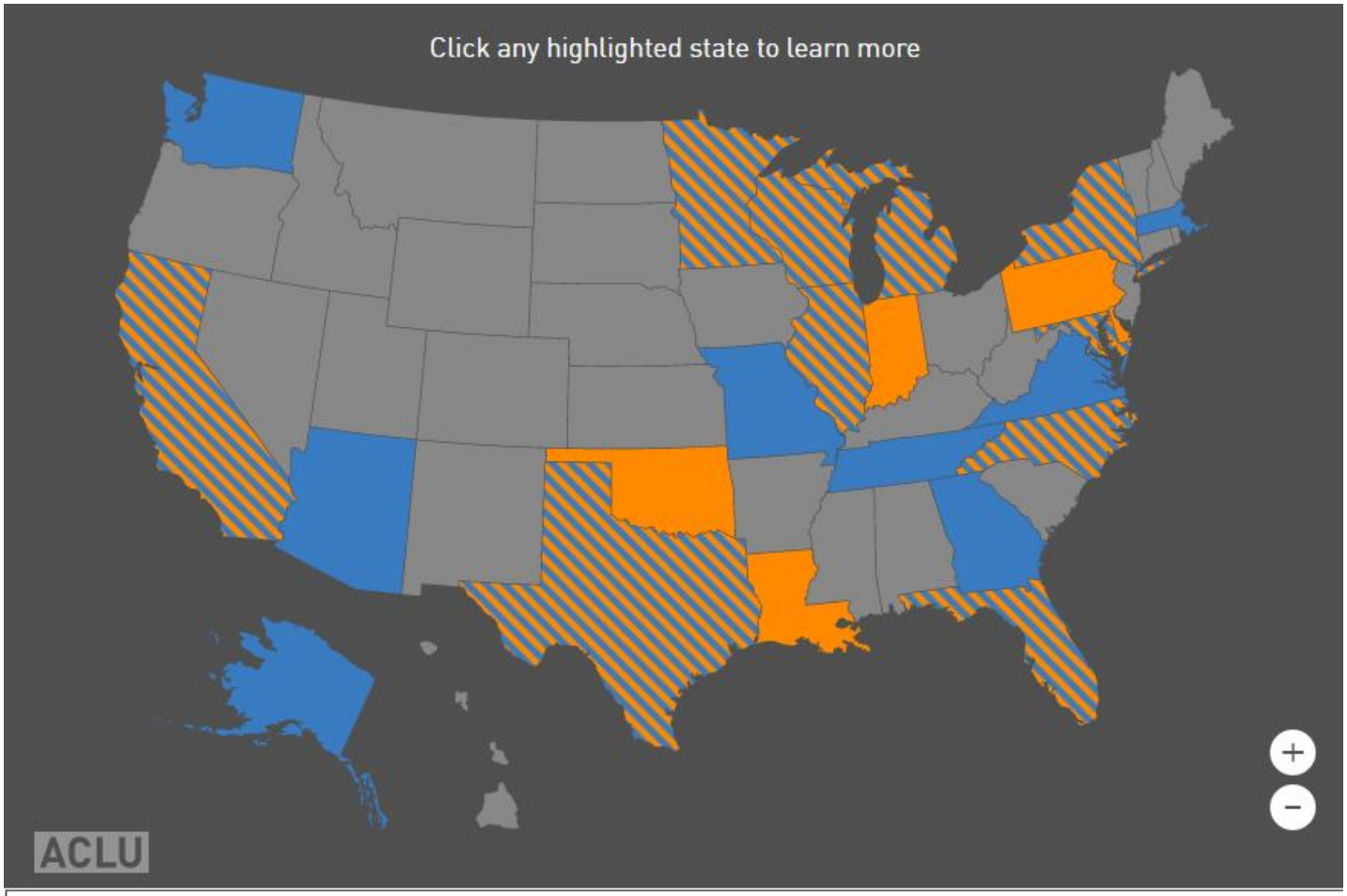
- **Other Name(s):** Cell-site simulators; International mobile subscriber identity (IMSI) catchers.

- **Function(s):** It mimics a cell phone communications tower, causing your cell phone to communicate with it. This communications link gives the Stingray the ability to track your location and intercept data from your phone, including voice and typed communications.

ACLU
AMERICAN CIVIL LIBERTIES UNION of MISSISSIPPI

Stingrays

- **Issue(s):**
  - When it grabs information off a targeted phone, it also sweeps in information about 100s or 1,000s of additional non-targeted phones.
  - The technology is often used without a warrant, or pursuant to a warrant issued by a judge who has been misled about what technology is being used or what its capabilities and limitations are
  - It is very difficult to detect when it is being used and to ensure that it is not being deployed in a discriminatory manner.



ACLU
AMERICAN CIVIL LIBERTIES UNION of MISSISSIPPI

Stingrays: A Guide for Public Defenders

- What kind of court authorization, if any, does the government currently obtain to use the device?
  - No court authorization?
  - Pen register/trap and trace order?
  - Hybrid Order?
  - Warrant?
- What guidance have courts offered on Stingrays?

Stingrays: A Guide for Public Defenders

- How can you tell if the government used a Stingray in your case?
  - Terminology
  - How did the government find out your client's cell phone number?
  - How did the government locate your client?
- What guidance have courts offered on Stingrays?

For more information, contact:

Blake Feldman: bfeldman@aclu-ms.org

or read more on our website at:

www.aclu.org/issues/privacy-technology

ACLU
AMERICAN CIVIL LIBERTIES UNION of MISSISSIPPI

www.aclu-ms.org